Purposefully Miscalibrated Atomic Counters for Mutating One-Time-Pad Systems for Robust Private Key Encryption

12 June 2024

Simon Edwards
Research Acceleration Initiative

Introduction

The advent of the novel atomic timekeeping apparatus known as an Optical-Atomic Stable Isotope Chronometer opens up the possibility of the use of unique, uncalibrated clocks (not used so much as clocks but rather as counters) in order to make possible the distribution of endless numbers of future private keys on the basis of the continued functioning of a pair of identically calibrated such timer arrays; one possessed by an operator and the other by the entity wishing to keep in contact with their operator.

Abstract

As OASIC-based timekeeping may be based on a wide variety of stable elements and any atomic clock may be based upon, for example, the averaging of multiple nodes in order to improve accuracy, atomic counters may be applied for purposes of cryptography rather than timekeeping. Much as the Enigma Machine used unique wheels in order to set keys, a single atom of a variety of natural elements can be creatively made to act as such wheels.

If one's object was not merely to keep accurate time, but rather to generate a series of arbitrary values (large numbers) which remain consistent between two physically segregated devices, the natural elements, themselves, offer a solution.

There are dozens of available stable isotopes of known elements, all of which would, in an OASIC regime, undergo quasi decay associated heating events at a predictable rate which are, of course, measurable by bolometer. Given a library of, for example, 50 elements (of which nine would be used in a given device) and nine "counters" which work in tandem with a properly calibrated atomic timekeeping node, one could generate unique strings each segment which would have 50^9 possible unique dynamics relative to the starting point. If each node were femtosecond-accurate, one might note the nine values from the -micro, -nano, -picosecond (excluding -femto in case of loss of accuracy) segments (at the top of each whole second, for example) and combine these values into a coherent string which is then run through an algorithm such as SHA-3 in order to produce a key.

These values would be unique to each hand-device and would vary depending upon time of activation of the hand-devices. The time of activation of the hand-devices would be known only to the entity issuing the device to the operator. The elements (and their sequence) in the counter devices would be known only to the issuer. The hand-device would be battery-powered and two batteries would be

used in order to ensure a constant supply of power (with one being changed at a time, as necessary.)

Encrypted messages would be transmitted to the operator with the time at which the cryptotext was generated transmitted in the clear. The operator would use the indicated time of message preparation in order to query the hand device as to the proper key of many stored keys to use for decryption. The hand-device would calculate and store a key once per second in solid-state memory and would have have a purposefully limited capacity for storing historical keys.

In the event that an operator becomes concerned that they are about to be compromised, they may remove the batteries from the device, which would cause the device to forget the time as well as trigger the erasure of stored keys. This would also trigger a mechanism which would physically void the contents of the monoatomic chambers containing the natural elements in order to deny this knowledge to an adversary attempting to reverse engineer the devices. Small compartments of pressurized air would blow the elements used clear of the device and contaminate the area around the monoatomic trap mechanism with the contents of a separate compartment featuring a single atom of each of the 50 elements used in the library sans the used element (as well as some not included in the library) in order to create maximal confusion upon forensic analysis. The loss of electrical power would trigger this final, sanitizing step as well as memory erasure. A particularly paranoid operator might add an additional fail-safe such as automated self-destruct triggered by failure to re-enter a safe condition code at least once per day. As the natural elements used in the device would not be known (nor knowable) to the operator, an operator under duress could not be forced to divulge this information, nor could they be forced to divulge the time of activation or the hashing algorithm used.

Conclusion

As it is frequently necessary for operators to transmit or receive large quantities of digital information (e.g. a digital photograph of a sensitive document or a photo of the interior of a secure area) the ability for two communicating parties to be able to agree in advance upon secure, private keys is an important ability. The most important pieces of information; time of activation and the elements used for the counters; could be readily be denied to an adversary in nearly all cases. As nine numbers derived from each of nine counters would provide a total of 81 pseudorandom yet mutually known numerical values which would subsequently be passed through a hashing algorithm which would ensure symmetrical distribution of values in the ultimate key, the requirements that keys not be re-used as well as that the key never be transmitted are met. Extant private key algorithms, both proprietary and open-source, could plausibly be used to secure larger quantities of data with a high level of confidence so long as the private key remains private.

Example:

Time of activation: 20241206 12:37:52.012.345.678.901.etc (unstored starting point)

Cleartext header from home base: 20241506 14:14:10.000.[000].[000].[000].000

Node 1 (Nitrogen): 612713612 Node 2 (Beryllium): 890183411 Node 3 (Argon): 908801310 Node 4 (Sulfur): 527059464 Node 5 (Neon): 871385713 Node 6 (Titanium): 095183492 Node 7 (Iron): 901234613 Node 8 (Manganese): 005163133 Node 9 (Silver): 783007372

Combined string extracted from counters at 14:14:10 is:

612713612890183411908801310527059464871385713095183492901234613005163133783007372

SHA-3 of above value =

fb15bf855fac69094993e42b43bdf7807226e4ab6b7a2a5d2db5f512332d82444bb9319e146be380836255a535a4ae16bc9e521387f7f9e8852c8c75a1a41759 and is therefore the encryption/decryption key indicated.